

ABSTRACT OF THE DISCLOSURE

An untrusted program is initially executed in a limited environment comprising mock resources. After execution, a diagnostic is run on the limited environment to determine whether the untrusted program exhibited any undesirable behavior (e.g. whether the untrusted program deleted, modified, renamed, etc. the mock resources). If undesirable behavior is detected, corrective action may be taken. Corrective action may include providing a warning to a user not to run the untrusted program in an unrestricted environment, and deleting the untrusted program. By prescreening an untrusted program in a limited and safe environment in this manner, it is possible to detect malignant programs and to prevent them from doing any real damage to a system.